GlobalResearch
Center for Research on Globalization

Wikileaks Vault 7 Highlights Importance of Tech Self-Sufficiency

By Ulson Gunnar

Global Research, March 12, 2017
New Eastern Outlook 11 March 2017

Region: USA
Theme: Intelligence

Leaked document clearinghouse Wikileaks has recently released an immense collection of documents detailing the US Central Intelligence Agency's (CIA) vast and literally Orwellian surveillance and spying capabilities.

The International Business Times in an article titled, "What's in Vault 7? WikiLeaks publishes huge trove of CIA secrets," would explain:

> WikiLeaks has revealed the contents of the long-awaited Vault 7 – a huge batch of documents allegedly detailing the hacking tools used by the US Central Intelligence Agency (CIA). The whistle-blowing organisation said it may be the largest intelligence publication in history.

It also stated that these tools were used across hacked platforms. It reported:

> This includes Samsung TVs, Microsoft Windows, Apple iPhones and smartphones using Google's Android operating system. The techniques could be used to give the CIA the ability "bypass the encryption" of WhatsApp, Signal, Telegram, Wiebo and Confide, WikiLeaks said.

In George Orwell's classic novel 1984, TVs would surveil the population, serving like a universal closed circuit television (CCTV) network. The incremental emergence of just such a surveillance state since the book's publication has often been described as "Orwellian." With devices such as phones, laptops, and smart TVs like those manufactured by Samsung now quite literally surveilling the public, the consequences warned of in Orwell's works have now become a reality.

While the revelations from Vault 7 suggest the US CIA and its European counterparts exploited commercial platforms to build its invasive spying network, some analysts have pointed out that many of these security exploits, backdoors and surveillance features have most likely been created with the explicit cooperation of large technology corporations.

Australia's Financial Review revealed in 2013 in an article titled, "Intel chips could let US spies inside: expert," that:

> One of Silicon Valley's most respected technology experts, Steve Blank, says

> he would be “surprised” if the US National Security Agency was not embedding “back doors” inside chips produced by Intel and AMD, two of the world’s largest semiconductor firms, giving them the possibility to access and control machines.

Corporations like Google and Facebook, the former of which created and maintains the above mentioned Android mobile operating system, openly collaborate with the United States government and the corporate and financial interests that dominate its domestic and foreign policy. It is highly likely, that in addition to assisting US special interests in the subversion of foreign nations and the facilitation of global war and instability, both corporations are also deeply involved in assisting in surveillance, spying and manipulating the public.

Decentralizing IT

The alliance between these special interests and technology corporations, particularly in light of this most recent deluge of leaked documents, highlights the fundamental importance of decentralizing the design, development, manufacturing and distribution of information technology.

Nations like Russia and China already find themselves in need of producing their own computer hardware and software. The use of domestically produced processors for government computers in Russia represents one tangible solution that can be used to overcome this obvious and growing problem.

Nations like Russia and China also have developed their own social media networks, search engines and even operating systems to protect their respective information spaces. Nations that rely on “security experts” from abroad often find themselves the victims of elaborate infiltration efforts that end up compromising their information space more than had they taken no measures at all.

Nations like Russia and China have entire pipelines through which human resources can be created and utilized for the construction of domestic information technology infrastructure and security. Other nations, particularly in the developing world must also create similar pipelines and organizations like Google and Facebook to dilute and displace the unwarranted influence these foreign tech giants have within their borders.

Likening IT security to national security, one would find it equally absurd to entrust the former to a foreign agency or enterprise. No nation would reasonably entrust the defense of their physical borders to an outside military force, so why entrust the security of their information space to similarly foreign organizations? Yet that is precisely what is happening around the world.

The CIA’s overreaching power as described in the Vault 7 leaks is only possible because of the vast reach of each and every platform the US intelligence agency used in constructing its techno-panopticon. Corporations like Samsung, Microsoft, Apple and Google reach into virtually every nation on Earth where information technology is prevalent, creating a virtual sea for the CIA’s sharks to swim through and hunt in. Draining this sea through decentralizing the control these corporations currently enjoy, vastly limits the hunting grounds the CIA has access to.

Despite Vault 7 making this unpleasant reality a matter of public debate and concern, being aware of such vast abuses made possible by equally vast tech monopolies is not enough. Nations and individuals creating alternatives beyond the reach of the CIA and other agencies and entities like it is essential in rolling back or at least complicating these invasive efforts.

Similar threats to privacy and security exist both across the growing "cloud" online, as well as throughout the growing physical network known as the "Internet of Things." And while both currently consist of likewise monopolized services and platforms, there is no reason why decentralized services and platforms cannot be used instead. Designers and developers around the world already have created and have made available (many times for free) such alternatives allowing people to create their own cloud servers and services as well as their own private "Internet of Things," independent of universal networks agencies like the CIA have likely infiltrated and compromised.

As a matter of national policy, governments around the world, outside of and targeted by the US-Euro surveillance network must make IT security as much a priority today, in the modern age of information and computing, as conventional armies, navies and air forces have been in protecting a nation's physical territory.

Ulson Gunnar, a New York-based geopolitical analyst and writer especially for the online magazine "New Eastern Outlook".

The original source of this article is New Eastern Outlook

Articles by: Ulson Gunnar

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

For media inquiries: publications@globalresearch.ca